



UNIVERSIDAD
POLITÉCNICA
DE MADRID

PROCESO DE
COORDINACIÓN DE LAS
ENSEÑANZAS PR/CL/001



E.T.S. de Ingeniería de
Sistemas Informáticos

ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

615001021 - Seguridad De Las Tecnologías De La Información

PLAN DE ESTUDIOS

61CD - Grado En Ciencia De Datos E Inteligencia Artificial

CURSO ACADÉMICO Y SEMESTRE

2023/24 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos.....	1
2. Profesorado.....	1
3. Conocimientos previos recomendados.....	2
4. Competencias y resultados de aprendizaje.....	2
5. Descripción de la asignatura y temario.....	3
6. Cronograma.....	5
7. Actividades y criterios de evaluación.....	7
8. Recursos didácticos.....	9
9. Otra información.....	11

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	615001021 - Seguridad de las Tecnologías de la Información
No de créditos	6 ECTS
Carácter	Obligatoria
Curso	Segundo curso
Semestre	Cuarto semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	61CD - Grado en Ciencia de Datos e Inteligencia Artificial
Centro responsable de la titulación	61 - Escuela Técnica Superior De Ingeniería De Sistemas Informáticos
Curso académico	2023-24

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Giannicola Scarpa (Coordinador/a)		g.scarpa@upm.es	- -

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

- Matemática Discreta I
- Matemática Discreta II
- Algoritmos Y Estructuras De Datos

3.2. Otros conocimientos previos recomendados para cursar la asignatura

El plan de estudios Grado en Ciencia de Datos e Inteligencia Artificial no tiene definidos otros conocimientos previos para esta asignatura.

4. Competencias y resultados de aprendizaje

4.1. Competencias

CE09 - Capacidad para describir los requisitos de seguridad de la información e implementar las medidas de seguridad informática necesarias para garantizar el acceso restringido y seguro a los datos y al conocimiento.

CG04 - Capacidad para innovar y encontrar soluciones creativas en situaciones complejas o de incertidumbre en el ámbito de la ingeniería.

CG06 - Identificar y utilizar las tecnologías de la información y las comunicaciones más adecuadas en el ámbito de la ingeniería.

4.2. Resultados del aprendizaje

RA88 - Seguridad de los Datos de carácter Personal

RA83 - Arquitectura de Seguridad y de Red frente a incidencias y ataques.

RA87 - Conocer, comprender y saber utilizar servicios criptográficos para la obtención de seguridad

RA85 - Conocimiento actualizado de soluciones de seguridad para la Sociedad de la Información

RA86 - Fundamentos de criptografía y criptoanálisis

RA82 - Conocer y comprender la importancia de la seguridad para la empresa

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

El objetivo de esta asignatura es hacer comprender a los alumnos el papel central que tienen los algoritmos y las estructuras de datos en la seguridad de los sistemas informáticos. Con ella se pretende que el alumno adquiera destrezas fundamentales en el uso, programación e implementación de algoritmos y sistemas que proporcionen seguridad a las TIC. Para ello el alumno habrá que aplicar conocimientos e intuición en el diseño de soluciones válidas según requisitos de seguridad especificados.

El objetivo global es que el alumno pueda llegar a diseñar, desarrollar y evaluar la Seguridad de sistemas, aplicaciones y servicios informáticos de todo tipo. Los conocimientos adquiridos siempre apuntarán al desarrollo, despliegue, organización y gestión de servicios informáticos en contextos empresariales que realmente puedan mejorar los procesos de negocio. En esta asignatura se favorecerá la capacidad del alumno en la resolución de problemas de seguridad recurriendo a los conocimientos que sean necesarios (matemáticas, ciencias, ingeniería, etc.).

Al final, el alumno conocerá y comprenderá la importancia que tiene la seguridad informática para las Administraciones y Empresas, serán capaces de identificar riesgos y posibles ataques. Para ello conocerá, comprenderá y sabrá utilizar servicios criptográficos para proporcionar seguridad TIC y conocerá algunas soluciones de seguridad que están disponibles y son válidas para la protección de la Sociedad de la Información.

5.2. Temario de la asignatura

1. Criptografía

- 1.1. Conceptos y Origen de la Criptografía
- 1.2. Soluciones Criptográficas y Métodos de Sustitución
- 1.3. Transposición y Máquinas de Cifrado
- 1.4. Criptoanálisis Clásico
- 1.5. Algoritmos de Cifrado Actuales
- 1.6. Funciones Hash
- 1.7. Criptografía Asimétrica

2. Aplicaciones

- 2.1. Software seguro
- 2.2. Código malicioso
- 2.3. Medidas Anticódigo Malicioso
- 2.4. Cortafuegos y SPDI
- 2.5. Control de acceso
- 2.6. Kerberos y Servicios de Autenticación
- 2.7. PGP y S/MIME
- 2.8. TLS e IPsec

3. Librerías criptográficas

- 3.1. Uso de librerías criptográficas como OpenSSL, GnuPG, o similares.

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			
2	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			
3	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			
4	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			
5	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			
6	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			
7	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			
8	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			
9	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			Ejercicio Individual Evaluación Progresiva del Bloque I del Temario EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 01:00
10	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			
11	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			
12	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			
13	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			

14	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			
15	Clases de teoría Duración: 04:00 LM: Actividad del tipo Lección Magistral			Ejercicio Individual Evaluación Progresiva del Bloque II del Temario EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 01:00
16				
17				Examen de Toda la Asignatura No- Aprobada previamente mediante Evaluación Progresiva EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 02:00

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso derivadas de la situación creada por la COVID-19.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
9	Ejercicio Individual Evaluación Progresiva del Bloque I del Temario	EX: Técnica del tipo Examen Escrito	Presencial	01:00	50%	0 / 10	CE09 CG04 CG06
15	Ejercicio Individual Evaluación Progresiva del Bloque II del Temario	EX: Técnica del tipo Examen Escrito	Presencial	01:00	50%	0 / 10	CE09 CG04 CG06

7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Examen de Toda la Asignatura No-Aprobada previamente mediante Evaluación Progresiva	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	0 / 10	CE09 CG04 CG06

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen Teorico de toda la asignatura	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	0 / 10	CE09 CG04 CG06

7.2. Criterios de evaluación

La evaluación progresiva de esta asignatura estará organizada en dos ejercicios individuales obligatorios.

Los ejercicios SUSPENSOS de Evaluación Progresiva deberán volverse a examinar en la prueba presencial de la Convocatoria Ordinaria.

La nota final de la asignatura será la media aritmética de las mejores calificaciones obtenidas en cada bloque tanto si se ha examinado en Evaluación Progresiva como en la Convocatoria Ordinaria.

Las pruebas obligatorias son dos exámenes en los que el alumno deberá responder correctamente y por escrito a las preguntas y enunciados que se le planteen. Estos exámenes se celebrarán en las fechas establecidas para ello en el calendario de la asignatura y disponibles en cada momento.

En el caso de no aprobarse la asignatura y tener que concurrir al examen de la Convocatoria Extraordinaria, el alumno/a tendrá que examinarse de todo el temario. No se guardan resultados entre convocatorias.

La puntuación correspondiente a cada examen por Evaluación Progresiva (Bloque I y Bloque II) supondrá un 50% de la nota final del alumno.

Es criterio de evaluación es la correcta respuesta a las preguntas planteadas a cada alumno, así como correcta satisfacción de los objetivos marcados en cualquier ejercicio práctico individual que se le plantee.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Cryptography and Network Security. Principles and Practice.	Bibliografía	5th Edition, William Stallings (Author) ISBN-10: 0136097049 ISBN-13: 978-0136097044
Applied Cryptography. Protocols, Algorithms, and Source Code in C	Bibliografía	2nd Edition, Bruce Schneier (Author) ISBN-10: 0471117099 ISBN-13: 978-0471117094
Practical Cryptography	Bibliografía	Niels Ferguson (Author), Bruce Schneier (Author) ISBN-10: 0471223573 ISBN-13: 978-0471223573
Handbook of Applied Cryptography. Discrete Mathematics and Its Applications	Bibliografía	Alfred Menezes, Paul van Oorschot y Scott Vanstone (Editores) ISBN-10: 0849385237 ISBN-13: 978-0849385230
Cryptography for Developers	Bibliografía	Tom St Denis (Author) ISBN-10: 1597491047 ISBN-13: 978-1597491044
BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic.	Bibliografía	Tom St Denis (Author) ISBN-10: 1597491128 ISBN-13: 978-1597491129
Codes, Ciphers, Secrets and Cryptic Communication. Making and Breaking Secret Messages from Hieroglyphs to the Internet,	Bibliografía	Fred B. Wrixon (Author) ISBN-10: 1579124852 ISBN-13: 978-1579124854
The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography,	Bibliografía	Simon Singh (Author) ISBN-10: 0385495323 ISBN-13: 978-0385495325
The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet,	Bibliografía	David Kahn (Author) ISBN-10: 0684831309 ISBN-13: 978-0684831305

Security in Computing	Bibliografía	(4ª ed.). Charles P. Pfleeger y Shari Lawrence Pfleeger. Prentice Hall (2006) ISBN-10: 0132390779, ISBN-13: 978-0132390774
Network Security: Private Communication in a Public World	Bibliografía	(2ª ed.). Charlie Kaufman, Radia Perlman y Mike Speciner. Prentice Hall (2002) ISBN-10: 0130460192, ISBN-13: 978-0130460196
Computer Security Basics	Bibliografía	(2ª ed.). Rick Lehtinen y G.T. Gangemi. O'Reilly Media, Inc. (2006) ISBN-10: 0596006691, ISBN-13: 978-0596006693
Computer Security	Bibliografía	(2ª ed.). Dieter Gollmann. Wiley (2006) ISBN-10: 0470862939, ISBN-13: 978-0470862933
Introduction to Computer Security.	Bibliografía	Matt Bishop. Addison-Wesley Professional (November 5, 2004) ISBN-10: 0321247442, ISBN-13: 978-0321247445
Fundamentals Of Computer Security	Bibliografía	Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry ISBN: 3540431012, ISBN-13: 9783540431015, 978-3540431015. Springer 2003

9. Otra información

9.1. Otra información sobre la asignatura

La asistencia a clase no es obligatoria y el comportamiento de los asistentes deberá ser respetuoso y correcto con todos los demás.

El alumno deberá colaborar en el adecuado desarrollo de las clases y demás actividades formativas del curso.

Antes de acudir a una tutoría, el alumno deberá solicitar cita para ello con el profesorado mediante un correo electrónico indicando tal interés.

El profesorado de la asignatura se reserva la potestad de dividir o reunir grupos para el desarrollo de temas específicos si el desarrollo del temario y sus actividades asociadas así lo aconsejan.

Si el desarrollo de la asignatura así lo requiriese o aconsejase, el profesorado de reserva la potestad de cambiar el orden en el que se exponen y desarrollan los distintos bloques que constituyen el temario de la asignatura.

Para el correcto desarrollo de esta asignatura, todos los alumnos deberán utilizar la plataforma Moodle en la que están registrados automáticamente como consecuencia de su matrícula en ella.

Está prohibido el plagio tanto en las memorias, como en los códigos o en el software que se desarrolle. En todos los casos el alumno deberá indicar explícitamente y con detalle de dónde han salido y cuál es el origen de los materiales que utiliza.

Está prohibida la mera traducción de artículos académicos o de cualquier otra índole. El uso de traductores automáticos está completamente prohibido.

Las incorrecciones sintácticas, ortográficas y semánticas del lenguaje utilizado podrán ser penalizadas.

Cualquier sospecha sobre la autoría de un examen, un ejercicio individual o una práctica, llevará inexorablemente al Examen Oral de la asignatura y parte del cuál será la defensa de lo expuesto en su entrega (examen, memoria, código, ejecutables, etc.).

